FCW.COM

Biometrics takes on physical access

Agencies have multiple ID options for bolstering building security

BY John Moore
Published on March 7, 2005

Government officials seeking to reinforce building and facility security are taking a closer look at biometrics. The technology employs physical characteristics such as a fingerprint or an iris scan to validate a person's identity.

The Defense Department, intelligence agencies and Energy Department laboratories have been using biometrics for years to secure facilities.

What's new, however, is a growing interest in biometrics among a broader government audience. In this era of heightened security, more agencies are concluding that traditional protective measures, such as identification badges and the like, may not be enough to keep facilities safe. Biometric tools increasingly fill the security gap.

An array of biometric systems may be enlisted for physical security. Hand geometry and fingerprint recognition already have found wide deployment, but newer technologies are vying for attention. Depending on the solution, the price of biometrically securing an entry can range from hundreds of dollars to more than $4,000.

But experts advise biometric buyers to look beyond the initial price tag before making a commitment. "You don't just look at the cost of hardware," said Dale Murray, tech team lead for the Entry Control and Biometrics Group at Sandia National Laboratories.

"In general, variables to consider include fast throughput, high reliability, ease of use and the cost for acquiring, installing and maintaining the technology," said John Woodward, director of DOD's Biometrics Management Office.

Increasing interest

Sandia, considered DOE's lead lab for security systems, has a history in the government's biometric adoption. The lab's initial foray into designing biometric systems dates back to the mid-1980s. But despite this early start, the adoption of biometrics for physical security has been gradual. Murray said people have approached the technology tentatively.

This trepidation, however, has begun to fade. For one, security employees are becoming more familiar with the technology. But the greater impetus comes from homeland security concerns. "With all this interest in homeland security, we've seen a strong uptick in interest," Murray said.

Indeed, vendors report that government customers are starting to recognize the limitations of traditional access- control measures. The problem with ID badges, radio frequency ID or proximity cards is that they provide single-factor authentication, said Ken Scheflen, senior vice president and general manager at Viisage, a biometrics vendor.

Security guards or card readers might recognize that a user's credential is valid, but they couldn't verify that the credential actually belongs to the user. Someone could have stolen a card or badge from its owner.

Organizations that rely on flash pass systems "pretty much have no security," Scheflen said. "What they have to move toward is…a multifactor system."

Such a system might require the use of a card, a personal ID number and a biometric identifier. "We like to think of it as three layers," said Joya Gooden, a project manager at STG. The company is assessing the physical security requirements of the Transportation Department's Volpe National Transportation Systems Center.

Policy initiatives might also compel agencies to pay more attention to biometrics. Homeland Security Presidential Directive 12, issued in August 2004, calls for a federal standard for secure and reliable forms of identification to protect facilities.

"It is going to bring access control to many government offices that in the past may not have had any," said Bill Spence, director of marketing at Recognition Systems. National Institute of Standards and Technology officials are working on a standard, called Personal Identity Verification, that will comply with the directive.

That standard, the release of which was imminent at press time, is expected to address biometrics. "So far, only fingerprints offer the combination of reliability, open standards and interoperability among products of different manufacturers necessary to the [Personal Identity Verification] standard," according to a NIST report released in January.

Biometric choices

Agency officials pursuing multifactor authentication have a few biometric options, including hand geometry, which is among the oldest and most widely used biometric technologies.

Hand geometry uses an individual's hand characteristics to verify identities. Recognition Systems' HandReaders, for example, take more than 90 hand measurements including length, thickness and surface area, according to the company.

Hand geometry has been around since the late 1960s and appeals to customers looking for a track record. "There's a lot of case history," said Erik Bowman, a systems engineer and program manager for biometrics at Northrop Grumman Information Technology. He adds that physical access control is the primary application for hand geometry.

Speed is one attribute of hand geometry and a significant reason the technology is installed in high-traffic areas. The hand geometry verification process takes less than one second, according to Recognition Systems. That speed minimizes user frustration.

"If you're standing at a door and trying to go through it, a second seems like an eternity," Spence said. "Any delay is significant."

Cost and size are potential drawbacks for hand geometry, industry executives say. A single reader can cost $3,000. The units tend to be larger than other types of biometric scanners, which could be an issue in some environments.

Fingerprint scanning is another prevalent technology. Michael Parks, director of homeland security operations at STG, cited fingerprint scanning and hand geometry as the most commonly used biometrics in government for physical access control.

Fingerprint recognition technology typically uses an optical device to scan fingerprints. The method is speedy, and the scanners are small and relatively inexpensive, with some turnkey systems priced around $1,000.

Northrop Grumman officials have installed a considerable number of fingerprint-scanning devices, Bowman said. But limitations exist. The glass platen on which users place their fingers can become dirty, obscuring the optical scanner.

Organizations with smokers, for example, may find that the platen acquires a yellow discoloration, Bowman said, adding that this will degrade the unit over time. The platen, however, can be replaced for a nominal fee.

Among other biometric tools, voice recognition has a following in the intelligence community, Parks said. Like hand geometry, the development of voice recognition spans several decades.

The up-and-comers

New biometric technologies continue to emerge. Facial recognition is among the hottest areas of development, Murray said. The approach is seen as more natural and less invasive than other biometrics. "A lot of people are comfortable with the concept," he said.

Facial recognition systems use the geometry of the human face to verify identity. To date, facial recognition has mostly been used in situations in which databases of facial images exist. Police departments, for example, use facial recognition in booking systems to determine if a suspect has been arrested before, Scheflen said. Motor vehicle departments use the technology to verify claimed identities. The same technology may also be used in physical access control, industry watchers said.

Iris recognition represents another rising technology and one that industry analysts consider among the most accurate. The method relies on the unique pattern of an individual's iris. Woodward said DOD installations — such as the Biometrics Management Office's Biometric Fusion Center in Clarksburg, W.Va. — have begun installing iris-recognition systems as the devices become more commercially available.

On the civilian side, Environmental Protection Agency officials have deployed Iridian Technologies' iris-recognition gear to help secure more than 60 doors in the agency's regional office in Dallas, said Jerry Ruddle, global vice president of sales and marketing at the company.

Cost may be an obstacle to adoption, however. "Iris scanning is only used in specialized security situations because of its relatively high cost and cumbersome equipment," according to a January industry report from the equity research arm of Janney Montgomery Scott.

Environmental factors must also be taken into consideration when deploying iris recognition. Direct sunlight can foil the iris scanner, as it can other biometrics using optical scanners.

"Bright sunlight into any camera has an effect on what image is acquired," Ruddle said. But he added it is a straightforward task to position the iris-recognition equipment so sunlight isn't a factor.

Industry executives advise buyers to weigh the pros and cons of biometric tools before making a decision. "There's no silver bullet biometric technology we can use and is perfect and will work in any environment," Spence said. "Each biometric technology has advantages and disadvantages."